The following information was posted with the attached DRAFT document:

May 28, 2015

NIST IR 8062

DRAFT Privacy Risk Management for Federal Information Systems

NIST requests comments on the draft report NISTIR 8062, *Privacy Risk Management for Federal Information Systems*, which describes a privacy risk management framework for federal information systems. The framework provides the basis for establishing a common vocabulary to facilitate better understanding of - and communication about - privacy risks and the effective implementation of privacy principles in federal information systems.

Please send comments to privacyeng <at> nist.gov by **July 13, 2015** at 5:00pm EDT using the comment matrix provided (link provided below).

Background:
Expanding opportunities in cloud computing, big data, and cyber-physical systems are bringing dramatic changes to how we use information technology. While these technologies bring advancements to U.S. national and economic security and our quality of life, they also pose risks to individuals' privacy.

Privacy Risk Management for Federal Information Systems (NISTIR 8062) introduces a privacy risk management framework for anticipating and addressing risks to individuals' privacy. In particular, it focuses on three privacy engineering objectives and a privacy risk model. To develop this document, NIST conducted significant public outreach and research. We are soliciting public comments on this draft to obtain further input on the proposed privacy risk management framework, and we expect to publish a final report based on this additional feedback.

Note to Reviewers:
To facilitate public review, we have compiled a number of topics of interest to which we would like reviewers to respond. Please keep in mind that it is not necessary to respond to all topics listed below, Reviewers should also feel free to suggest other areas of revision or enhancement to the document.

- *Privacy Risk Management Framework:* Does the framework provide a process that will help organizations make more informed system development decisions with respect to privacy? Does the framework seem likely to help bridge the communication gap between technical and non-technical personnel? Are there any gaps in the framework?
- *Privacy Engineering Objectives:* Do these objectives seem likely to assist system designers and engineers in building information systems that are capable of supporting agencies' privacy goals and requirements? Are there properties or capabilities that systems should have that these objectives do not cover?
- *Privacy Risk Model:*

o Does the equation seem likely to be effective in helping agencies to distinguish between cybersecurity and privacy risks?

o Can data actions be evaluated as the document proposes? Is the approach of identifying and assessing problematic data actions usable and actionable?

o Should context be a key input to the privacy risk model? If not, why not? If so, does this model incorporate context appropriately? Would more guidance on the consideration of context be helpful?

o The NISTIR describes the difficulty of assessing the impact of problematic data actions on individuals alone, and incorporates organizational impact into the risk assessment. Is this appropriate or should impact be assessed for individuals alone? If so, what would be the factors in such an assessment

NISTIR 8062 (Draft)

Privacy Risk Management for Federal Information Systems

Editors:

Sean Brooks
Ellen Nadeau

Authoring Committee:

Michael Garcia
Naomi Lefkovitz
Suzanne Lightman

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8062 (Draft)

Privacy Risk Management for Federal Information Systems

Editors:

Sean Brooks
Ellen Nadeau

Authoring Committee:

Michael Garcia
Naomi Lefkovitz
Suzanne Lightman

Information Technology Laboratory, NIST

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8062
64 pages (May 2015)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: privacyeng@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This document describes a privacy risk management framework for federal information systems. The framework provides the basis for the establishment of a common vocabulary to facilitate better understanding of and communication about privacy risks and the effective implementation of privacy principles in federal information systems. This publication focuses on the development of two key pillars to support the application of the framework: privacy engineering objectives and a privacy risk model.

Keywords

Privacy; Information Security; Risk Management; Cybersecurity; Computer Security

Acknowledgements

The authors wish to thank the following individuals for participating in the preparation of this document: James Dever, Simson Garfinkel, Meredith Jankowski, and Colin Soutar. The authors also greatly appreciate the NSTIC pilots' generous contribution of time and insights.

Table of Contents

Executive Summary

NIST research in several areas of information technology – including cybersecurity, Smart Grid, cloud computing, big data, and cyber-physical systems – improves the products and services that bring great advancements to U.S. national and economic security and our quality of life. Notwithstanding their benefits, public awareness about these technologies and their potential impact on individuals' privacy and societal values continues to grow. This publication lays the groundwork for greater understanding of privacy impacts and the capability to address them in federal information systems through risk management.

Federal agencies need methods that yield repeatable and measurable results if they are to be able to implement privacy protections in information systems in a consistent manner. Although existing tools such as the Fair Information Practice Principles (FIPPs) and privacy impact assessments (PIAs) provide a foundation for taking privacy into consideration, they have not yet provided a method for federal agencies to measure privacy impacts on a consistent and repeatable basis.

In other domains such as cybersecurity, safety, and finance, risk management has played a key role in enabling agencies to achieve their mission goals while minimizing adverse outcomes. NIST has successfully developed frameworks to assess risk, including the management of cybersecurity risk through the Risk Management Framework (RMF). Modeled after the RMF, this publication introduces a privacy risk management framework (PRMF). In developing the PRMF, NIST sought the perspectives and experiences of privacy experts across a variety of sectors in an open and transparent process, including hosting workshops and public comment periods and engaging stakeholders in various outreach activities.

The PRMF provides the basis for the establishment of a common vocabulary to facilitate better understanding of, and communication about, privacy risks and the effective implementation of privacy principles in federal information systems. In particular, this publication focuses on the development of two key pillars to support the application of the PRMF: privacy engineering objectives and a privacy risk model.

Privacy engineering objectives can play an important role in bridging the gap between an agency's goals for privacy and their manifestation in information systems. NIST has developed three privacy engineering objectives – *predictability, manageability, and disassociability* – for the purpose of facilitating the development and operation of privacy-preserving information systems. These objectives are designed to enable system designers and engineers to build information systems that implement an agency's privacy goals and support the management of privacy risk.

A critical aspect of risk management is a risk model that enables the ability to identify risk. Risk is often expressed as a function of the likelihood that an adverse outcome occurs multiplied by the magnitude of the adverse outcome should it occur. This publication examines this conception of risk and how it can be expressed in terms that facilitate improved identification and management of privacy risk. To aid agencies in using the PRMF and to apply the privacy risk model, NIST has developed an initial set of worksheets, collectively referred to as the Privacy Risk Assessment Methodology (PRAM). This document describes the inputs to the PRAM, and provides examples for agencies to follow when applying the PRAM to their own systems.

Future areas of work in privacy risk management will focus on improving the application of controls – policy, operational, and technical – to mitigate risks identified with the PRMF. To facilitate this research, NIST will continue to request feedback to refine the privacy engineering objectives and the privacy risk equation, and to develop additional guidance to assist agencies in determining the likelihood and impact of privacy risks. The research process will continue to be an open and transparent process that will solicit input from federal agencies, academic institutions, private organizations, and civil society organizations in order to develop guidance that reflects the best practices for addressing privacy risks.

1. Introduction

NIST research in information systems has identified the value of measurable and repeatable methods for anticipating and addressing risks in the use of information technology. Among these risks are those involving individuals' privacy. This publication lays the groundwork for greater understanding of privacy impacts and the capability to address them in federal information systems through risk management.

Purpose

This publication introduces a privacy risk management framework (PRMF) for anticipating and addressing privacy risk that results from the processing of personal information in federal information technology systems. In particular, this publication focuses on the development of two key pillars to support application of the PRMF: privacy engineering objectives and a privacy risk model. In so doing, it lays the foundation for the establishment of a common vocabulary to facilitate better understanding of, and communication about, privacy risks and the effective implementation of privacy principles in federal information systems.

The set of privacy engineering objectives defined in this document provides a conceptual framework for engineers and system designers to bridge the gap between high-level principles and implementation. The objectives are intended to support privacy risk management by facilitating consistent, actionable, and measurable design decisions.

The privacy risk model aims to provide a repeatable and measurable method for addressing privacy risk in federal information systems. The model defines an equation and a series of inputs designed to enable (i) the identification of problems for individuals that can arise from the processing of personal information and (ii) the calculation of how such problems can be reflected in an organizational risk management approach that allows for prioritization and resource allocation to achieve agency missions while minimizing adverse events for individuals and agencies collectively.

Scope

This publication covers the assessment of privacy risk arising from the processing of personal information within and among information systems. The PRMF is intended to aid agencies in identifying and prioritizing risk so they can implement the appropriate mitigations. It provides system objectives to facilitate privacy engineering, a common vocabulary, and a risk equation for assessing privacy in information systems.[1]

The PRMF described herein does not address the processing of personal information outside of information systems. It also does not examine specific controls or their applicability to specific privacy risks. A future document will explore in greater detail controls that an agency could use to mitigate privacy risk in information systems.

Audience

Addressing privacy is a cross-organizational challenge that requires agencies to use a common language to describe privacy risk and the objectives they wish to pursue in order to manifest privacy protections within the information systems they manage. This document provides a common vocabulary for these discussions, as well as some preliminary tools for estimating privacy risk. Thus, the audience for this document is all positions involved in the development of information systems, the evaluation of privacy risk in such systems or risk management in general, including:

- Individuals with privacy and/or information system oversight responsibilities (e.g., senior agency officials for privacy, chief information officers, agency heads);
- Individuals with privacy implementation and operational responsibilities in information systems (e.g., mission/business owners, information system owners, information owners/stewards, system administrators, information system security officers);
- Individuals with system engineering and design responsibilities (e.g., program or project managers, system engineers, chief architects); and
- Individuals with oversight and/or accountability responsibility for privacy (e.g., inspectors general, internal auditors).

[1] Privacy engineering is an emerging field, but currently there is no widely-accepted definition of the discipline. For the purposes of this publication, privacy engineering is a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within information systems.

Document Organization

This publication is organized as follows:

The remainder of **Chapter 1** explains the need for a privacy risk management framework by reviewing current concerns about the impact of information technologies on individuals' privacy, existing tools to address privacy protection and their challenges, and NIST privacy engineering research to date.

Chapter 2 explores the use and benefits of risk management in cybersecurity, and discusses its relevance to the privacy field.

Chapter 3 introduces the privacy risk management framework. It defines three privacy engineering objectives and a privacy risk model expressed as a privacy risk equation. It introduces a privacy risk assessment methodology based on the equation to enable federal agencies to identify and calculate privacy risk in their systems.

Chapter 4 explains the next steps for privacy risk management work at NIST. It stresses the importance of continued research in the field of privacy engineering and the need for more guidance on the application of controls to mitigate privacy risk.

This document also includes eight appendices:

- Appendix A is a glossary of terms used throughout this document;
- Appendix B is a list of acronyms used throughout this document;
- Appendix C provides a formal mathematical statement of the privacy risk model;
- Appendix D contains a set of worksheets and illustrative data maps that comprise the privacy risk assessment methodology;
- Appendix E is a catalog of problematic data actions for use with the privacy risk assessment methodology;
- Appendix F is a catalog of problems for individuals for use with the privacy risk assessment methodology; and
- Appendix G is an illustrative set of contextual factors for use with the privacy risk assessment methodology;
- Appendix H includes a list of references used throughout the document.

Background

Defining the need

NIST research in several areas of information technology – including cybersecurity, Smart Grid, cloud computing, big data, and cyber-physical systems – improves the products and services that bring great advancements to U.S. national and economic security and our quality of life. Notwithstanding their benefits, public awareness about these technologies and their potential impact on individuals' privacy and societal values continues to grow.

For example, during its work with Smart Grid technology, NIST and its partners in the electricity sector have noted that there are significant privacy implications. "While many of the types of data items accessible through the smart grid are not new, there is now the possibility that other parties, entities or individuals will have access to those data items; and there are now many new uses for and ways to analyze the collected data, which may raise substantial privacy concerns."[2] Energy data and personal information collected by smart grids "can reveal something either explicitly or implicitly about individuals, groups of individuals, or activities of those individuals."[3]

Other examples of emerging technologies in which the federal government is facing privacy concerns are cyber-physical systems (CPS) and the Internet of Things (IoT). IoT and CPS will have major impacts in areas such as transportation, medicine, critical manufacturing, and energy. The public working groups that NIST has convened on CPS and big data included privacy as a major research area.[4]

Many of these issues converge in the particular privacy challenges governments are confronting as they implement "smart city" technologies, such as managed traffic flow and automated ticketing (i.e. red light and speed cameras) that can collect information about people through "government-operated sensors and surveillance technologies increasingly deployed throughout their environs."[5] Use, retention, and storage of this type of data have raised citizen concerns about privacy infringement.[6]

[2] NIST Interagency Report 7628R1 "Guidelines for Smart Grid Cybersecurity,: Volume *II*, p.2 – Privacy and the Smart Grid," (SEPT 2014) at 7, *available at* http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf [hereinafter NISTIR 7628R1].

[3] *Id.* at 25.

[4] *See* "Cyber-Physical Systems Public Working Group Workshop," NIST Homepage, accessed May 19, 2015, *available at* http://www.nist.gov/cps/cps-pwg-workshop.cfm; NIST Special Publication 1500-4, "DRAFT NIST Big Data Interoperability Framework: Volume 4, Security and Privacy," (APRIL 2015) *available at* http://bigdatawg.nist.gov/_uploadfiles/M0395_v1_4717582962.pdf

[5] Kelsey Finch and Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 Fordham Urban L. J. 1581, 1595 (2015), *available at* https://www.dropbox.com/s/nw1nbf1uj6kq2zw/Finch%20-%20Tene_Cities.pdf?dl=0.

[6] For discussions regarding the myriad privacy issues involved in "smart city" technologies, *see* Nicole Perlroth, *Smart City Technology May Be Vulnerable to Hackers*, NY Times, Apr. 21, 2015, *available at* http://bits.blogs.nytimes.com/2015/04/21/smart-city-technology-may-be-vulnerable-to-hackers/; Reid Wilson, *Red-light Cameras Under Scrutiny In State Legislatures*, Wash. Post, Feb. 7, 2014, *available at*

As NIST conducts research in these and other information technologies and federal agencies deploy them, it is critical to understand the potential impacts for privacy, so that they can be addressed. Doing so will enable the optimization of the benefits of these technologies while maintaining core values provided by the protection of individuals' privacy.

Existing Privacy Tools and Challenges

As a result of these ubiquitous privacy concerns, NIST guidelines and reports increasingly feature privacy considerations.[7] To date, these efforts to address privacy have generally been based on privacy principles such as the Fair Information Practice Principles (FIPPs).[8] Principles such as the FIPPs have helped many organizations develop baseline considerations for the protection of individuals' privacy as new technologies enter the marketplace. Nonetheless, there are ongoing debates about the adaptability of these principles to new technologies.[9]

These debates may have less to do with the FIPPs as concepts of enduring value and more to do with the metaphorical problem of forcing a square peg into a round hole. That is, agencies need methods that yield repeatable and measurable results if they are to be able to implement privacy protections in information systems on a consistent basis. There are a number of reasons why the FIPPs, notwithstanding their conceptual value, do not have the characteristics of a repeatable and measurable methodology. One is that there

http://www.washingtonpost.com/blogs/govbeat/wp/2014/02/07/red-light-cameras-under-scrutiny-in-state-legislatures/; Luke Broadwater, *City Surveillance Camera System to Expand*, Baltimore Sun, July 21, 2012, *available at* http://articles.baltimoresun.com/2012-07-21/news/bs-md-ci-private-cameras-20120721_1_security-cameras-crime-cameras-citiwatch-system; Jay Stanley, *Extreme Traffic Enforcement*, American Civil Liberties Union, May 24, 2012, *available at* https://www.aclu.org/blog/extreme-traffic-enforcement; and Phineas Baxandall, *New Report Outlines Problems with Red-Light and Speed Cameras*, The Federation of Public Research Interest Groups, Oct. 27, 2011, *available at* http://www.uspirg.org/trafficcamreport.

[7] *See e.g.*, NISTIR 7628R1, *supra* Note 2; NIST Special Publication 800-53R4 "Security and Privacy Controls for Federal Information Systems and Organizations," (APR 2013), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; and NIST "Framework for Improving Critical Infrastructure Cybersecurity," (FEB 2014) *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[8] The FIPPs first appeared in a 1973 report by the U.S. Department of Health, Education, and Welfare and addressed privacy concerns arising from the increasing digitization of data. *See* "Records Computers and the Rights of Citizens," at 41-42, *available at* http://www.justice.gov/opcl/docs/rec-com-rights.pdf. After publication, the FIPPs became influential in shaping privacy law in the United States and around the world. Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy* 114 Colombia L. Rev. 583, 592 (2014), *available at* http://columbialawreview.org/wp-content/uploads/2014/04/Solove-Hartzog.pdf. The FIPPs were embodied in the Privacy Act of 1974, 5 U.S.C. § 552a, *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.

[9] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," (MAY 2014), at 21, *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

can be wide-ranging interpretations about their meaning. For instance, the transparency FIPP can be treated as a requirement that mandates that individuals be provided with specific notices about the collection and use of their information. In other instances, transparency is more akin to a value statement about the importance of open processes. Another important reason is that the application of the FIPPs is centered on the purpose or reason that personal information is being used. Since the purpose could be broad, a FIPP such as data minimization does not inherently assist an agency in determining which information should be minimized to mitigate risk.[10] Additionally, the FIPPs are usually treated as a unified set even though they may operate at different levels of the organization. For example, the accountability and auditing FIPP constitutes concepts that are generally applicable to a number of policy domains, not just privacy, and which are typically considered as part of an overall organizational governance framework, not necessarily at the systems engineering level. Thus, for system engineers, the FIPPs, on their own, do not offer a consistent methodology that yields repeatable results for the protection of privacy.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is one example of an initiative that demonstrates both the value of the FIPPs and their challenges.[11] The NSTIC acknowledged that federated identity solutions could create risks for individuals' privacy and civil liberties as such solutions could increase the capability for tracking and profiling of online transactions.[12] It calls for a holistic implementation of the FIPPs to enable a privacy-enhancing identity ecosystem.[13] NIST has awarded grants to pilots that demonstrate alignment with the guiding principles laid out in the NSTIC.[14] The pilots' use of the FIPPs has generally resulted in solutions that improve individual notice and consent, data security, and policy-based use limitations.[15] However, they lag in identification of the risks around tracking and profiling created by architectural design choices or selection of technical controls to mitigate such risks.[16] Thus, these pilots have often sought help from NIST in conducting privacy evaluations and assessments of their risk for both internal and external reporting purposes.

[10] The FIPPs are not a risk-based framework because they do not frame privacy harms according to the actual impact on individuals. *See* Stuart S. Shapiro, PhD., "Situating Anonymization Within a Privacy Risk Model," Homeland Security Systems Engineering and Development Institute (2012) at *2, *available at* https://www.mitre.org/sites/default/files/pdf/12_0353.pdf.

[11] *See generally* "National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy," (APR 2011), *available at* https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[12] *Id.* at 3.

[13] *Id.* at 12.

[14] "Catalyzing the Marketplace: NSTIC Pilot Program," NSTIC Homepage, accessed May 19, 2015, *available at* http://www.nist.gov/nstic/pilots.html.

[15] NIST Internal Report 8054 "NSTIC Pilots: Catalyzing the Identity Ecosystem," (APR 2015), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8054.pdf.

[16] To address this issue and other challenges associated with the NSTIC principle of privacy enhancing identity solutions, NIST announced its Federal Funding Opportunity in March 2015, *available at* http://www.nist.gov/nstic/NSTIC-Privacy-Pilot-FFO-03-2015.pdf.

Agencies, because they are required to implement privacy impact assessments (PIAs) under the E-Government Act of 2002, have the basis for a tool to facilitate repeatable and measurable privacy protections in their systems.[17] In practice though, PIAs have not achieved their full potential as a process for assessing and understanding (and therefore anticipating) privacy concerns in information systems.[18] Where agencies focus largely on using them to support regulatory compliance, it can be difficult to translate the information in PIAs into actionable technical design recommendations. Enabling agencies to better define privacy risk and system objectives for privacy could expand the utility of PIAs and their benefits as a tool for addressing privacy concerns in federal information systems.

New Tools to Address the Challenges

The FIPPs and other related principles remain an important part of an overall privacy protection framework.[19] However, experiences with the NSTIC pilots and other NIST efforts have demonstrated that although principles can provide important considerations for policy development, they need to be supplemented with additional tools that facilitate repeatable and measurable methods for identifying, prioritizing, and mitigating privacy problems. Given the lack of such tools, NIST determined that developing a consistent process for addressing privacy concerns in information systems would be beneficial for internal NIST work and federal agency missions.

Other disciplines (e.g., cybersecurity, safety, finance) have successfully used risk management approaches to unify multiple organizational inputs and drive toward a common assessment of challenges and identification of solutions.[20] NIST has successfully developed frameworks to assess risk in a variety of disciplines, including the cybersecurity risk management model, which particularly informed the approach

[17] The E-Government Act of 2002 is codified at 44 U.S.C. § 101, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm.

[18] For instance, in the healthcare context, the Centers for Medicare & Medicaid Services developed and documented PIAs yet did not assess the risks associated with the handling of PII or identify mitigating controls to address such risks. United States Government Accountability Office "Healthcare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls," (SEPT 2014), at 44, *available at* http://www.gao.gov/assets/670/665840.pdf.

[19] *See e.g.*, Privacy by Design principles, Ann Cavoukian, PhD., et al., "Privacy Engineering: Proactively Embedding Privacy, by Design," Information and Privacy Commissioner Ontario, Canada, (JAN 2014), at 2-3, *available at* https://www.privacybydesign.ca/content/uploads/2014/01/pbd-priv-engineering.pdf.

[20] *See generally* NIST Special Publication 800-37R1 "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle," (FEB 2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf; United States Government Accountability Office "High Risk Series: An Update," (FEB 2015), *available at* http://www.gao.gov/assets/670/668415.pdf; and
Federal Aviation Administration "System Safety Process Steps," (JAN 2005), *available at* https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/media/ssprocdscrp.pdf.

developed in this report.[21] These risk management frameworks facilitate management decisions about conducting business processes, achieving legal compliance, allocating resources, and setting system controls. In general, agencies can more systematically align their work with their mission and objectives if they have a consistent method for assessing risk.

In the privacy field, a number of organizations including MITRE, the Centre for Information Policy Leadership, the iMinds-DistriNet research group at the University of Leuven, and others have published recent work highlighting the importance of understanding privacy risk in improving privacy-preserving system engineering.[22] Many of these organizations have specifically cited a need for a risk model for privacy. None of these organizations, however, has proposed a complete privacy risk model. [23] Therefore, the first step in developing privacy engineering practices within federal agencies is to establish a framework for identifying privacy risks and their impact on organizational goals. With such a framework, agency officials may more effectively direct organizational resources toward the mitigation of identified privacy risks while supporting the mission of their agencies.

NIST Privacy Risk Management Framework Development Process

In developing the PRMF, NIST sought the perspectives and experiences of privacy experts across a variety of sectors in an open and transparent process, including hosting workshops, holding public comment periods, and engaging stakeholders in various outreach activities in a broad range of fora.

NIST held three public events in April, September, and October of 2014. The first two were in Gaithersburg, Maryland, and San Jose, California, respectively; the third was an interactive webcast. At the April workshop, NIST led discussions focusing on organizational privacy challenges. The workshop also evaluated risk models in other disciplines – such as cybersecurity – and their potential to inform similar work in privacy.

[21] *See e.g.,* NIST 800-37R1, *supra* Note 20; NIST Special Publication 800-39 “Managing Information Security Risk: Organization, Mission, and Information System View,” (MAR 2011), at 8, *available at* http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf; and NIST Special Publication 800-30R1 “Guide for Conducting Risk Assessments,” (SEPT 2012), *available at* http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[22] *See generally* Stuart S. Shapiro, PhD. et al., “Privacy Engineering Framework,” MITRE Corporation (AUG 2014), *available at* http://www.mitre.org/publications/technical-papers/privacy-engineering-framework; Centre for Information Policy Leadership, “Risk-based Approach to Privacy: Improving Effectiveness in Practice” Hunton & Williams LLP (JUN 2014), *available at* https://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf; and LINDDUN: A Privacy Threat Assessment Framework, *available at* https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf.

[23] Notably, the World Economic Forum has highlighted how security risk models are inappropriate for understanding the full nature of privacy risk. World Economic Forum, “Rethinking Personal Data: A New Lens for Strengthening Trust,” (May 2014), at 18, *available at* http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

In addition to the 240 stakeholders that attended the workshop in person, over 100 people attended via webcast. These participants spanned a wide variety of sectors representing the legal, policy, and technical aspects of privacy. In the April 2014 workshop, attendees identified the following key issues, which helped NIST focus its attention on the development of privacy engineering objectives and a risk model:

1. There is a communication gap around privacy between the legal and policy, design and engineering, and product and project management teams that increases the difficulty for organizations to manage privacy concerns effectively, understand risks and implement mitigating controls before harm occurs. A contributing factor is the lack of a common vocabulary and set of tools that can be used to build consistent requirements and technical standards across agencies.
2. There is a need for more development tools that measure the effectiveness of privacy practices.
3. Risk management should be a fundamental driver of an agency's approach to privacy.

The second workshop had over 130 in-person attendees and an additional 500 participants during the October 5th webcast. At this workshop and during the webcast, participants reviewed and discussed NIST's initial draft of the privacy engineering objectives and an information system privacy risk model.[24] Following the September workshop, NIST held an open comment period on these objectives and requested additional feedback. Numerous organizations responded to the call for comments, including major technology companies, civil society organizations, trade associations, and federal agencies.[25]

NIST has conducted other outreach over the past year, spreading awareness about the privacy risk management work while engaging stakeholders from across the fields of privacy and cybersecurity. This outreach has consisted of formal presentations to a number of key federal stakeholders, including the privacy committee of the U.S. Government's Chief Information Officers Council, the National Privacy Research Forum of the Networking and Information Technology Research and Development (more commonly known as NITRD) program, and the NIST Information Security and Privacy Advisory Board. NIST has presented to numerous academic institutions, federal agencies, trade associations and other stakeholders from private industry, and advocacy organizations. Through this outreach, NIST has received feedback from a wide array of stakeholders, better informing the development of the privacy risk methodology and the supporting materials. This publication sets forth a refined version of the framework originally presented in the September 2014 workshop and reflects feedback received in workshop discussions, public comments and outreach.

[24] The NIST workshop "Privacy Engineering Objectives and Risk Model Discussion Draft" is *available at* http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf.

[25] *See* "Comments on Privacy Engineering Objectives and Risk Model," NIST Homepage, accessed May 20, 2015, *available at* http://csrc.nist.gov/projects/privacy_engineering/public_comments.html.

2. Risk Management & its Applicability to Privacy

Risk management is a comprehensive process that enables organizations to achieve their mission goals while minimizing adverse outcomes. A risk management framework helps agencies to better identify, assess, and mitigate risk to their organization. It assists in determining which activities are most important to assure critical operations and service delivery. In turn, these determinations aid agencies in prioritizing investments and maximizing the impact of each dollar spent. By providing a common language to address risks present in a field, risk management is especially helpful in communicating inside the organization (e.g. across management levels and operating units), as well as outside the organization. A risk management framework specifically for privacy can help agencies to address privacy risk within their broader enterprise risk portfolio to improve these outcomes.

Risk Management

Enterprise risk management encompasses:

- Aligning risk strategy
- Enhancing risk response decisions
- Reducing operational surprises and losses
- Identifying and managing multiple and cross-enterprise risks
- Seizing opportunities
- Improving deployment of capital

http://www.coso.org/default.htm

NIST has successfully developed frameworks to assess risk, including the risk management framework for management of cybersecurity risk(s) (RMF).[26] The RMF has several characteristics that make it a useful model for informing the PRMF as it:

- concentrates on information systems;
- has well-established objectives, and it has a significant level of maturity;
- is not law or regulation-based, but can facilitate legal compliance because it does not pre-suppose any particular policy or outcome and is technology-neutral; and
- can enable the setting of appropriate controls to mitigate potential issues.[27]

The PRMF models the following key components:

- characteristics or properties of secure systems;[28]
- a common vocabulary for describing cybersecurity risk; and

[26] NIST 800-37R1, *supra* Note 20; *see also* NIST 800-39, *supra* Note 21; and NIST 800-30R1, *supra* Note 21.

[27] *See generally* NIST 800-37R1, *supra* Note 20.

[28] *Id.* at 2. For further information regarding the characteristics of secure systems to include security objectives, *see* NIST Federal Information Processing Standards Publication Series 199 "Standards for Security Categorization of Federal Information and Information Systems," (FEB 2004), at 1-2 *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. The security objectives are codified in FISMA: "integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity…confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information…availability, which means ensuring timely and reliable access to and use of information." 44 U.S.C. § 3542, *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2008-title44/pdf/USCODE-2008-title44-chap35-subchapIII-sec3541.pdf.

- an equation to enable the calculation of cybersecurity risk for a given system.

NIST research suggests that equivalent components would be beneficial for the management of privacy risk, as privacy risks have not been comprehensively addressed by cybersecurity risk management.[29] In contrast to cybersecurity, impacts on individuals are intrinsic to notions of privacy.[30] These impacts have generally been classified under the concept of privacy invasions, but are referred to in this document more simply as problems.[31]

As noted above, the underlying rationale for risk management is the achievement of mission goals while minimizing adverse outcomes or problems. With respect to individuals and information systems, the privacy problems that they may experience arise from the processing of their personal information. That is to say, when information systems are conducting operations that, for example, involve collecting, generating, using, storing, or disclosing information about individuals, these activities can give rise to the kinds of problems described in the catalog in Appendix F.[32] To understand how cybersecurity risk management and privacy risk management are complementary, but distinct processes, agencies must consider the source of these problems. While the source may be unauthorized access to systems that contain information about individuals, problems can also arise from information processing operations of the systems themselves. For example, in the energy sector, some communities have responded negatively to smart meters due largely to concern that utilities' collection of the information itself can reveal people's behavior inside their homes, not from concerns that the utilities cannot keep the information secure.[33] Moreover, even actions taken to protect personal information can have privacy implications. For example, security tools to defend personal information from malicious actors, such as persistent activity monitoring, can

[29] *See* United States Government Accountability Office "High-Risk Series: An Update," (FEB 2015), at *2, *available at* http://www.gao.gov/assets/670/668415.pdf wherein the challenges to ensuring the privacy of personally identifiable information in the face of rapidly changing technology is underscored.

[30] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. Rev. 477, 484 (2006), *available at* https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf.

[31] As Daniel J. Solove explains, the concept of "privacy" is a vague notion. Accordingly, he developed a useful privacy taxonomy wherein he focused on the specific activities that pose privacy problems for individuals. *Id.* at 481-82.

[32] NIST developed this non-exhaustive catalog to enable the validation of the PRMF. The catalog is derived from Daniel Solove's, *A Taxonomy of Privacy. Supra* Note 30.

[33] Chris Hooks, *As Towns Say No, Signs of Rising Resistance to Smart Meters*, New York Times, May 18, 2013, *available at* http://www.nytimes.com/2013/05/26/us/as-texas-towns-say-no-signs-of-rising-resistance-to-smart-meters.html?_r=0; Federico Guerrini, *Smart Meters: Between Economic Benefits and Privacy Concerns*, Forbes, June 1, 2014, *available at* http://www.forbes.com/sites/federicoguerrini/2014/06/01/smart-meters-friends-or-foes-between-economic-benefits-and-privacy-concerns/; Samuel J. Harvey, *Smart Meters, Smarter Regulation: Balancing Privacy and Innovation in the Electric Grid*, 61 UCLA L. Rev. 2068, 2076-90 (2014), *available at* http://www.uclalawreview.org/pdf/61-6-10.pdf**.** For a discussion regarding privacy risks weighed against big data opportunities, *see* Jules Polonetsky and Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 Stan. L. Rev. 25 (2013), *available at* http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf.

create similar concerns about the degree to which information is revealed about individuals that is unrelated to cybersecurity purposes.

A privacy risk management framework, therefore, should provide the capability to assess the risk of problems for individuals arising from the operations of the system that involve the processing of their information. Cybersecurity risk management frameworks, standards, and best practices can be used to address risks to individuals arising from unauthorized access to their information. Thus, NIST assumes that an agency implementing the PRMF in this publication will already be using a cybersecurity risk-based approach to manage such risks. Used in conjunction with a cybersecurity risk management framework, the PRMF proposed in this document offers a consistent, repeatable process for evaluating and enabling communication of privacy risk to facilitate the implementation of law, policy, and regulation aimed at protecting the totality of individuals' privacy.

3. NIST Privacy Risk Management Framework

The PRMF enables an agency to determine the sources of privacy risk to individuals in an information system. An agency can repeat these processes consistently across departments, providing comparable results. An agency can use this framework to first identify its goals and obligations for privacy protection, assess its systems against these governing requirements, prioritize mitigation mechanisms, and monitor for changes.

The NIST RMF categorizes four broad processes in looped phases, as illustrated in *Figure 01*: (i) *frame* risk (i.e., establish the context for risk-based decisions); (ii) *assess* risk; (iii) *respond* to risk once determined; and (iv) *monitor* risk on an ongoing basis.[34]

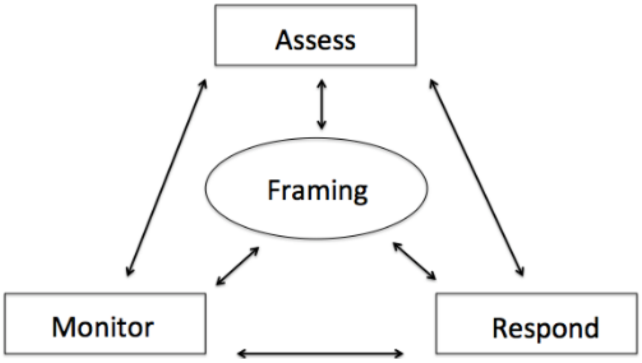


Figure 01: NIST Risk Management Framework

Building on these four phases, the NIST PRMF is composed of six processes that are tailored for addressing privacy in information systems.

The six processes are:

- **Frame business objectives**. An agency frames the business objectives for its system, including the agency needs served. Such needs may include the demonstration of specified privacy-preserving functionality. This process will support the end-stage design and implementation of controls because appropriate controls must permit the system to achieve the intended business functions while demonstrating measurable results for privacy protection.
- **Frame organizational privacy governance**. An agency frames the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals, and other commitments within which the system must operate. This process is a key input into the calculation of privacy risk as it allows better assessment of the impact of identified problems for individuals arising from the processing of their personal information on organizational privacy requirements and goals. Such an impact assessment is necessary for agencies to be able to use risk management to achieve their missions while minimizing adverse events for individuals and agencies collectively.
- **Assess system design.** To assess system design from a privacy perspective, agencies will need to describe the lifecycle of the system operations with respect to the personal information being processed by that operation and specific contextual factors that may heighten or lower the risk potential of the system operation. This process documents the inputs necessary for the privacy risk

[34] NIST 800-39, *Supra* Note 21 at 8.

model. It provides a method for making the concerns of individuals visible to agencies and how these concerns correlate to the behavior of the system.

- **Assess privacy risk.** In this stage, an agency identifies and prioritizes privacy risks. The process integrates the inputs from the previous three stages so that agencies can use the privacy risk model to calculate and prioritize the privacy risk of specific operations of their systems. This prioritization enables agencies to determine appropriate resource allocations to address the risks.
- **Design privacy controls.** Having prioritized risk in the previous phase, this phase is focused on the selection and implementation of controls to mitigate identified privacy risks. The design process includes selection and implementation to enable the development of tools and guidance for increasing agency awareness of the full spectrum of available controls, including technical measures that may supplement or improve upon existing policy-centric controls based on the FIPPs.[35]
- **Monitor change.** In this process, an agency assesses any changes in an information system that would impact individuals' privacy such as changes in system operations involving the processing of personal information, changes in the personal information being processed or changes in contextual factors, as well as monitoring the effectiveness of implemented privacy controls.

While the PRMF is unique because of its focus on privacy, the processes are similar to other types of risk frameworks.[36] The distinctive nature of the PRMF arises from its foundation on two key communication and analytical tools: the privacy engineering objectives and the privacy risk model described in greater detail below.

To aid agencies in using the PRMF and to apply the privacy risk model, NIST has developed an initial set of worksheets, collectively referred to as the Privacy Risk Assessment Methodology (PRAM). Appendix D contains drafts of worksheets that support processes one through four of the PRMF. As noted in the Scope section above, the selection and implementation of controls is an area of future work for NIST. NIST will continue to develop the PRAM to address phase five of the PRMF as this work evolves. The remainder of this document describes the privacy engineering objectives, the privacy risk model, and the inputs for the PRAM worksheets.

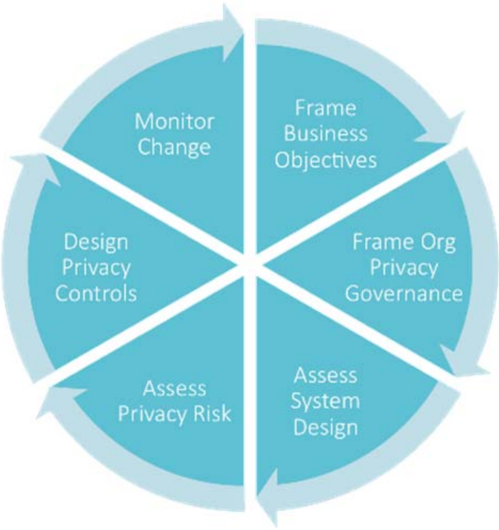


Figure 02: NIST Privacy Risk Management Framework

[35] *See* NIST 800-53R4, Appendix J, *supra* Note 7 at J-1.
[36] *See. e.g.,* NIST 800-30R1, *supra* Note 21.

System Objectives in Cybersecurity Risk Management

Following the workshop in April of 2014, NIST first focused its efforts on the communication gap cited by multiple attendees as being at the core of many of their organizations' privacy challenges.[37] A key question emerged that helped guide the examination of other fields that had successfully bridged this gap: what do other disciplines have that privacy does not? An examination of the cybersecurity field highlighted one potential avenue for exploration: objectives or system properties also known as confidentiality, integrity, and availability (CIA triad).[38]

The CIA triad was first articulated in 1975.[39] While initially designed to catalog different typologies of threats to information systems, with their ultimate codification in the Federal Information Security Management Act of 2002 ("FISMA"), CIA triad evolved to become a positive outcome-based model used to maintain security. This transition of the CIA triad from their use as broad threat classifications to characteristics of secure systems highlights what makes the security objectives useful to an agency.

The objectives provide a concrete way to think about security and target the points in systems where engineering needs to occur in order to enable a secure system. FISMA requires a risk management process for cybersecurity in federal systems.[40] Agencies must be able to communicate across various internal units (e.g., engineering, management, policy, legal, compliance) in order to highlight areas of risk, and determine how those risks impact other mission priorities. Objectives provide a tool in facilitating communication across these boundaries. While a senior official may not understand the technical implications of a particular cybersecurity risk, describing that risk in terms of the system's confidentiality, integrity, or availability can bridge that communication gap. An engineer may not understand the policies that dictate certain design requirements, but can understand how to develop a system if those requirements can be interpreted in terms of confidentiality, integrity, and availability.

As described above, agencies have been reliant on principles like the FIPPs that have provided a combination of values, governance principles, and requirements, but lack the concrete conceptualizations that the CIA triad has provided cybersecurity. The FIPPs

[37] The webcast of the April 2014 Privacy Engineering Workshop, held at the NIST offices in Gaithersburg, MD, is *available at* http://www.nist.gov/itl/csd/privacy-engineering-workshop-webcast.cfm.

[38] NIST Special Publication 800-14 "Generally Accepted Principles and Practices for Securing Information Technology Systems," (SEPT 1996), *available at* http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf, recognizes fundamental principles that should comprise an organization's information security program to include protecting the confidentiality, availability and integrity of the organization's data.

[39] *See* Jerome H. Saltzer, and Michel D. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE 63(9), pp. 1278-1308, 1975 at *2-3 *available at* http://www.acsac.org/secshelf/papers/protection_information.pdf.

[40] *See* 44 U.S.C. § 3541, *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2008-title44/pdf/USCODE-2008-title44-chap35-subchapIII-sec3541.pdf. NIST developed its Special Publication 800-30R1 as part of its FISMA Implementation program. *See* NIST 800-30R1, *supra* Note 21.

provide senior officials a foundation for considering privacy in information systems, but do not yield an approach for consistent communication of outcome-based aspects of a system that would enable engineers to assess their systems for appropriate capabilities and system design options. Privacy engineering objectives can play a key role in bridging the gap between an agency's goals for privacy and their manifestation in information systems.

Privacy Engineering Objectives

NIST has developed three privacy engineering objectives for the purpose of facilitating the development and operation of privacy-preserving information systems: predictability, manageability, and disassociability. These objectives are designed to enable system designers and engineers to build information systems that are capable of implementing an agency's privacy goals and support the management of privacy risk. As with CIA, these objectives are core characteristics of information systems. A system should exhibit each objective to some degree to be considered a system that could enable privacy protections while achieving its functional purpose.

***Predictability** is the enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.*

***Manageability** is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure.*

***Disassociability** is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.*

Predictability

Predictability provides agencies with both precision and flexibility in aligning their information systems to support privacy-preserving user relationships. A reliable belief about what is occurring with personal information in a system is core to building trust and enabling self-determination. These precepts have been the foundation of the transparency FIPP. By framing this objective in terms of reliable assumptions, agencies can begin to measure more concretely the expression of transparency in an information system. Enabling reliable assumptions does not require that individuals know all the technical details about how a system processes their personal information. Rather, predictability is about designing systems such that stakeholders are not surprised by the handling of personal information.[41] In this way, predictability can support a range of organizational interpretations of transparency from a value statement about the importance of open processes to a requirements-based view that specific information should be shared.

Predictability, however, is more than transparency. For system operators, predictability provides a broader base for control selection when assessing a system's privacy risk. Even in a system that may create unpredictable or previously unknown results – such as a large data analysis or research effort – predictability can provide a valuable set of insights about how to control privacy risks that may arise. For example, if the results of a data action are inherently unpredictable, operators can implement controls to restrict access to or use of those results. They can also consider technical controls that could de-identify individuals so that individuals can make reliable assumptions about when a system would reveal certain information about them and when it would not. A variety of controls, including technical controls, can facilitate implementation of predictability to produce the desired outcome for privacy.

Finally, predictability supports the translation or implementation of the FIPPs for use limitation and purpose specification in a manner that allows for innovation. For example, inherent in the rationale for use limitation is the recognition that changes in processing of personal information are loci for privacy risk. By focusing on maintaining reliable assumptions about that processing, predictability enables operators to assess the impact of any changes and target the application of appropriate controls. Thus, predictability facilitates the maintenance of stable, trusted relationships between information systems and individuals and the capability for individuals' self-determination, while enabling operators to continue to innovate and provide better services.

Manageability

Manageability is an important system property for enabling self-determination, as well as fair treatment of individuals. If agencies cannot administer individuals' information with sufficient granularity, they cannot be confident that inaccurate information can be identified and corrected, obsolete information is deleted, and only necessary information is collected or disclosed. In short, if the information system does not permit fine-grained control over data, agencies cannot implement key FIPPs, including maintaining data quality and integrity, achieving data minimization, and implementing individuals' privacy preferences.

Nonetheless, manageability is not a policy statement about the general right of individuals to control their information. It creates the system capability to manifest this policy, while minimizing potential conflicts in system functionality. For instance, it might

[41] See e.g., Pat Conroy et al., "Building Consumer Trust: Protecting consumer data in the consumer product industry," (NOV 2014), available at http://dupress.com/articles/consumer-data-privacy-strategies/ wherein Deloitte reported the results of its recent study of online consumers that showed 80% are "more likely to purchase brands from consumer product companies that they believe protect their personal information."

impair the functioning of some systems for individuals to be able to edit or delete information themselves (e.g., fraud detection or proof of eligibility). Manageability in these systems, however, would still enable the appropriately privileged actor to administer changes to maintain accuracy and fair treatment of individuals. Finally, manageability could support the mapping of technical controls such as data tagging and emerging standards in identity management that relate to attribute transmission.

Disassociability

Disassociability captures one of the essential elements of privacy-enhancing systems – that the system actively protects or "blinds" an individual's identity or associated activities from unnecessary exposure. Unlike confidentiality, which is focused on preventing unauthorized access to information, disassociability recognizes that privacy risks can result from exposures even when access is authorized or as a byproduct of a transaction.[42] Disassociability advances the capabilities of a privacy-preserving system by engaging system designers and engineers in a deliberate consideration of such points of exposure.

Although the operational requirements may vary depending on the system, achieving this objective should reflect the ability to complete the transaction without associating information to individuals. For example, identity proofing or the direct provision of health care services may necessitate the association of information with an individual. However, operational requirements should not include the mere difficulty of disassociating the information from individuals. Agencies may opt to accept the risk because of the difficulty in implementing appropriate controls or institute other compensating controls, but the recognition of such risk is distinct from defining specific associations of information as an operational requirement.

Many cryptographic techniques that exist today or are currently being researched could be mapped to disassociability.[43] The adoption of disassociability as an objective could not only raise awareness of the benefits of these techniques, but could increase demand for more advances. A further consideration for increasing the effectiveness of disassociability is whether a taxonomy could be constructed of existing identity-related classifications, including anonymity, de-identification, unlinkability, unobservability,

[42] Pursuant to 44 U.S.C. § 3542, *available at* http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf, confidentiality "means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information."

[43] For instance, the use of the "zero-knowledge proof" cryptographic method could allow one party (the prover) to authenticate an identity to another party (the verifier) without the exchange of private or secret information. *See* NIST Special Publication 800-21R2 "Guideline for Implementing Cryptography in the Federal Government," (DEC 2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf.

pseudonymity or others.[44] Such a taxonomy could potentially support more precise control mapping and risk mitigation.

Together, these three privacy engineering objectives, complemented by the CIA triad to address unauthorized access to personal information, provide a core set of information system capabilities to support the balanced attainment of agency business goals and privacy goals, and assist in the mapping of controls to mitigate identified privacy risks. Like the CIA triad, they provide a degree of precision and measurability, so that system designers and engineers, working with policy teams, can use them to bridge the gap between high-level principles and implementation within a functional system.

[44] Some of these concepts are explored in Draft NISTIR 8053 "De-Identification of Personally Identifiable Information," (APR 2015), *available at* http://csrc.nist.gov/publications/drafts/nistir-8053/nistir_8053_draft.pdf. *See also* LINDDUN: A Privacy Threat Assessment Framework, *available at* https://people.cs.kuleuven.be/~kim.wuyts/LINDDUN/LINDDUN.pdf which outlines a method for modeling privacy-specific threats.

A Privacy Risk Model

Risk is often expressed as a function of the likelihood that an adverse outcome occurs multiplied by the magnitude of the adverse outcome should it occur.[45] In information security, likelihood is understood as a function of the threats to the system, the vulnerabilities that can be exploited, and the consequences should those vulnerabilities be exploited.[46] Accordingly, security risk assessments focus on where in the system damaging events could cause problems. Excepting the issue of unauthorized access to personal information, privacy risk differs. As noted earlier, the adverse outcomes, or problems for individuals, can arise from the operations of the system itself, regardless of external factors and even in the absence of a technical vulnerability, such as poor software design or implementation. Thus, the terms "threat" and "vulnerability" fail to capture the essence of many privacy problems for individuals.

Data Actions

Data actions are information system operations that process personal information. "Processing" can include, but is not limited to, the collection, retention, logging, generation, transformation, disclosure, transfer, and disposal of personal information.

Consequently, a privacy risk model that can help organizations identify privacy risk as distinct from security risk requires terminology more suited to the nature of the risk. Given the focus on the operations of the system when processing personal information, an information system's privacy risk, therefore can be described as a function of the likelihood that a data action (a system operation processing personal information) causes problems for individuals, and the impact of the problematic data action should it occur. In simple terms, privacy risk can be expressed as:

$$\textbf{Privacy Risk} = \textbf{Likelihood of a problematic data action} \times \textbf{Impact of a problematic data action}$$

Using this new equation, agencies can calculate the privacy risk of a data action by assessing likelihood and impact of the data action becoming problematic. It is important to consider both of these factors, because neither one alone can aid an agency in prioritizing controls and allocating resources.

Likelihood is assessed as the probability that a data action will become problematic for a representative or typical individual whose personal information is being processed by the system. The PRAM demonstrates a step by step analysis of likelihood. Agencies can

[45] *See* NIST 800-30R1, *supra* Note 21 at 8-13.

[46] For an explanation of Information Technology risk assessments, *see* NIST Special Publication 800-100 "Information Security Handbook: A Guide for Managers," at 88-89, *available at* http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

support the assessment of likelihood in a number of ways. They may use existing information on customer demographics to estimate likelihood; they may extrapolate from information available about privacy concerns in similar scenarios; alternatively, they could conduct focus groups or surveys to glean more thorough and specific information from users about privacy concerns.

Impact is assessed as the magnitude of the problematic data action on the organization if it occurs. Impact is expressed through the organization for a few reasons. Although the purpose of the PRAM is to make more visible the problems that individuals can experience from the processing of their personal data in information systems, such problems may occur at some distance from the initial processing in the agency system. In addition, the actual magnitude for individuals may depend on their subjective experiences, such that an agency has to make a risk-based determination based on the composition of all individuals that may be affected. Finally, an important function of risk calculation is to produce a risk prioritization that can enable determinations about risk mitigation. Therefore, agencies must be able to reflect their best understanding of the problems individuals may experience through the lens of their overall mission needs, privacy-related goals and responsibilities, and resources. For this reason, the first two stages of the PRMF are processes that enable agencies to frame their mission needs and privacy goals and requirements. The PRAM reflects these framing processes with an impact analysis focused on four organizational impact factors, listed below with illustrative examples:

1. Noncompliance costs: how will the agency be impacted by not complying with applicable laws, policies, contracts, etc.?
2. Direct costs: will the agency face a decrease in use of the system or face other impediments to achieving its mission?
3. Reputational costs: how will this potential problem affect public trust in the agency?
4. Internal culture costs: how will employee morale, retention, or other aspects of agency culture be affected?

These four factors should not be considered an exhaustive list. Each agency should consider any additional impact factors specific to its work, mission, structure, and customer base.

Prioritization helps agencies to align mission priorities and resources. Addressing data actions with low likelihood and low impact of being problematic may be of a lower priority while addressing those with high likelihood and high impact is of the highest priority. However, likelihood and impact do not always align. For example:

- **Low likelihood/high impact:** While certain data actions may be less likely to become problematic, they could have a severe impact; in these cases, an agency may prioritize mitigation of these problems because any incidence of this severe problem would have unacceptable consequences. For example, if researchers had access to a data set of individuals' health information, the likelihood that the researchers would use the information improperly might be low, but the consequences for individuals, and therefore, for the mission and reputation of the organization, might be severe if misuse did occur, given the sensitive nature of health information.

- **High likelihood/low impact:** Alternatively, a problematic data action with a small impact may have a very high likelihood, leading an agency to prioritize controls for those problems in order to not negatively affect such a large portion of their constituents, even if the impact is low. For instance, an agency might use a web analytics tool that raised concerns among users of the website. In this case, the impact may be limited to some customer questions or complaints, but given that the tool affects all users, the agency might prioritize the application of a control that anticipates and addresses the concerns.

These prioritization decisions will vary by agency and data action, but are much better informed if both likelihood and impact are systematically assessed for each data action. In many cases, a determination of likelihood and impact may not be a simple process; just as implementing controls requires investment, properly assessing risk requires investment. In some cases conducting research may be necessary to better understand the likelihood of a privacy problem occurring. In others, it may be more appropriate to rely on the knowledge of experts in the agency. Agencies must consider the benefits and costs of different approaches.

Inputs to the Privacy Risk Assessment Methodology

This section describes the inputs set forth in the PRAM that are used in calculating likelihood and impact. The principal inputs are the data actions of the system, the personal information associated with a data action, and context, or the circumstances surrounding the data actions. This section also describes the analytical functions that agencies can apply to these inputs to enable risk prioritization so that they can make determinations about risk acceptance or mitigation. In future iterations, the PRAM may include the capability for agencies to compare controls for maximizing cost-effective mitigations.

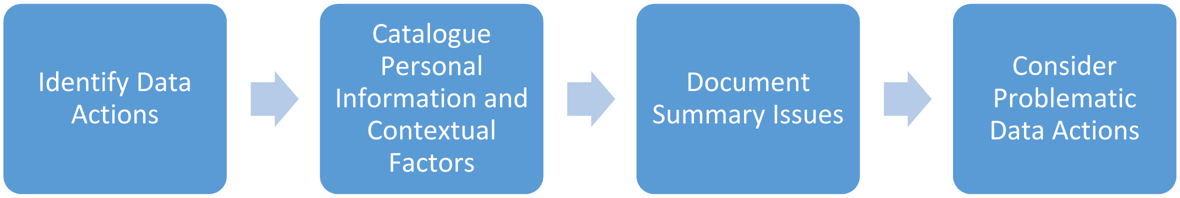

Identify Data Actions
Catalogue Personal Information and Contextual Factors
Document Summary Issues
Consider Problematic Data Actions

Figure 03: Inputs for the PRAM

Data Actions

Data actions are any information system operations that process personal information. As noted, the privacy risk model hinges on whether a data action becomes problematic for individuals. Thus, the PRAM is oriented around the analysis of specific data actions for privacy risk. To better analyze the context applicable to each data action's risk, agencies should map and describe data actions at a sufficiently granular level. For example, rather than using a high level label such as “collection” or “retention," agencies might include more descriptive details, such as “collection from users at registration via mobile device” or “storage in an internal database.”

Personal Information & Context

There are two critical inputs that modify the risk of any given data action: personal information and context. For each data action, an organization should identify the associated personal information at a granular level (e.g., doctor name, doctor address, and medical diagnosis instead of simply “health information”). Agencies should consider personal information broadly, and should include not only information that directly identifies an individual, but also information about events or behavior that can be linked to that individual.[47] As with data actions, granular mapping of personal information is important; it may be that specific pieces of personal information heighten the privacy risk, such that applying targeted controls may enable the agency to better preserve system functionality while mitigating risk to an acceptable level.

The risk of a data action is also a function of context – the circumstances surrounding the system's processing of personal information. An agency may need to consider context from various viewpoints (e.g., organizational, system, individual, data action) to determine which circumstances influence the risk of a data action.[48] Capturing contextual factors will likely require coordination between privacy officers and information technology personnel within an agency.

Summary Issues

Both context and associated personal information contribute to whether a data action has the potential to cause privacy problems. Based on these pieces of information, it is possible for an organization to draw initial observations about data actions - characterized as summary issues. Summary issues can be expressed as statements that upon further analysis heighten the assessment of risk or decrease it. They can also be expressed as questions that function as flags. Depending on the stage of system design, agencies may have open questions about certain aspects of the system operations. They should capture these open questions because the eventual determinations may be dispositive to the risk assessment. For example, whether a data action will be executed by the agency itself or a third-party may be undecided at an early stage of design, but the eventual disposition could be an important assessment factor. Therefore, the open question should be flagged until the determination is made, and the final assessment can be completed.

[47] For the purpose of risk assessment, personal information is considered broadly as any information that can uniquely identify an individual as well as any other information, events or behavior that can be associated with an individual. Where agencies are conducting activities subject to specific laws, regulation or policy, more precise definitions may apply.

[48] *See infra* catalog of contextual factors in Appendix G.

Problematic Data Actions

After cataloging the summary issues related to each data action, the next step of the analysis is to identify the adverse effects, or problems for individuals that could arise from these actions; these are termed problematic data actions. Each problematic data action could result in one or more potential problems for individuals. Understanding which problems are more likely to occur - and have the greatest impact - may help an agency to pinpoint what type of control would be most effective to mitigate a data action's privacy risk. For the validation of the PRAM, NIST has developed a non-exhaustive catalog of problematic data actions and problems set forth in Appendices E and F, respectively.

Once these inputs and analyses have been captured in the worksheets, agencies can use the PRAM to calculate the privacy risk of each data action. This process enables them to compare risk points within the system, and prioritize them. Thus, the PRAM provides a repeatable process that enables agencies to visualize where privacy risk may be occurring in their systems, communicate these risks at appropriate organizational levels, and make resource decisions with respect to addressing the risks.

4. Next Steps

It is NIST's goal that this PRMF may inform agencies about privacy risk the same way risk management frameworks for cybersecurity have informed the assessment and mitigation of security risks. As the understanding of cybersecurity risks has become more thorough, a baseline expectation for an understanding of this process has become common. As a result, much of what is formalized in cybersecurity risk management strategies like the NIST RMF has become second nature to many individuals contributing to the security of agencies' information systems. As NIST continues to research privacy engineering, it is our goal to provide a complete set of tools that agencies can use to understand potential privacy risks, prioritize them, and effectively address them.

To realize these goals, future areas of work in privacy risk management will focus on improving the application of controls – policy, operational and technical – to mitigate risks identified with the PRMF. It will require research to identify the breadth of controls available, what kinds of privacy risks they can address, how they can be effectively applied, and what kind of ancillary effects their application may create. To facilitate this research, NIST will continue to request feedback to refine the privacy engineering objectives and the privacy risk equation, and to develop additional guidance to assist agencies in determining the likelihood and impact of privacy risks. The research process will continue to be an open and transparent process that will solicit input from federal agencies, academic institutions, private organizations, and civil society organizations in order to develop guidance that reflects the best practices for addressing privacy risks.

Appendices

Appendix A: Glossary

Context: the circumstances surrounding the system's processing of personal information

Data Actions: Information system operations that process personal information.

Manageability: Providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure

Disassociability: Enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.

Personal Information: For the purpose of risk assessment, personal information is considered broadly as any information that can uniquely identify an individual as well as any other information, events or behavior that can be associated with an individual. Where agencies are conducting activities subject to specific laws, regulation or policy, more precise definitions may apply.

Predictability: Enabling of reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.

Privacy control: The administrative, technical, and physical safeguards employed within organizations to mitigate risks to individuals arising from the processing of their personal information within information systems.

Privacy engineering: Privacy engineering is an emerging field, but currently there is no widely-accepted definition of the discipline. For the purposes of this publication, privacy engineering is a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within information systems.

Problematic Data Actions: A data action that causes an adverse effect, or problem, for individuals.

Processing: Operation or set of operations performed upon personal information that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of personal information. See ISO/IEC 29100:2011(E) for a related definition.

Risk: A measure of the extent to which an entity or individual is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[49]

Summary Issues: Initial contextual analyses about data actions that may heighten or decrease the assessment of privacy risk.

[49] *See* NIST 800-30R1, *supra* Note 21 at 8-13.

Appendix B: Acronyms

CPS	Cyber-physical systems
FIPPs	Fair Information Practice Principles
IDP	Identity service provider
IoT	Internet of Things
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NSTIC	National Strategy for Trusted Identities in Cyberspace
OTP	One time password
PIA	Privacy impact assessment
PRAM	Privacy Risk Assessment Methodology
PRMF	Privacy Risk Management Framework
RMF	Risk Management Framework

Appendix C: Formal Mathematical Statement of the Privacy Risk Model

In this document, privacy risk is given by:

Privacy Risk	=	**Likelihood of a problematic data action**	x	**Impact of problematic data action**

If this is true for each data action in an information system, then the unmitigated privacy risk for an entire system, R_U, is given by

$$R_U = \sum_{d}^{D} \sum_{p}^{P} L_{dp} I_{dp}$$

where L_{dp} is the likelihood of privacy problem p occurring in data action d
I_{dp} is the impact of privacy problem p on the agency if it results from data action d
D is the set of all possible data actions
P is the set of all possible privacy problems.

Mitigated, or residual, agency privacy risk for a system, R_R, is given by

$$R_R = \sum_{d}^{D} \sum_{p}^{P} (L_{dp} - C_{dp}^{L})(I_{dp} - C_{dp}^{I})$$

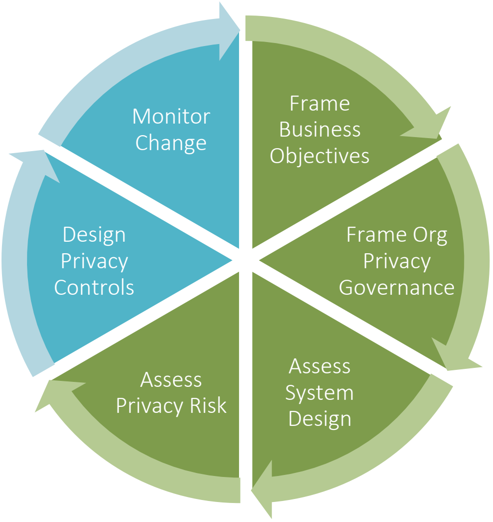
where C_{dp}^{L} is the reduction in likelihood of privacy problem p occurring in data action d by employing control C
C_{dp}^{I} is the reduction in impact of privacy problem p on the agency if it results from data action d by employing control C

The residual risk calculation implies that, for any data action, a given control can reduce the likelihood of a privacy problem, the impact of that privacy problem should it occur, or both. While controls are not the focus of this document, this outcome is sufficiently important to address here. When determining controls, the agency may be able to dynamically reduce privacy risk through a single control that reduces both likelihood and impact and, potentially, does so in multiple data actions.

Appendix D: Privacy Risk Assessment Methodology

Introduction

In order to better understand the practical implications of utilizing the privacy risk framework outlined in this document, NIST developed the PRAM. The PRAM consists of a series of worksheets that can be used to frame business objectives and privacy governance, and assess system design and privacy risk. These worksheets provide a practical method for implementing the framework. The current iteration only provides worksheets through the Assess Privacy Risk phase. As NIST develops the privacy risk framework further, it will explore how to best improve this tool, including developing worksheets to support the Design Privacy Controls phase.



A few of the funding recipients in the NSTIC pilot program have used this methodology while reviewing their systems for alignment with the NSTIC privacy guiding principle.[50] These pilots provided valuable insight into the practical application of this risk assessment methodology. Their size ranged from start-ups to large information technology companies, and included systems designed for private use as well as public service deployment. The maturity of the systems assessed also varied, and allowed NIST to understand the value of privacy risk assessment at different stages of technical development.

The worksheets catalog data actions, context, and other inputs of risk. The worksheets provided a baseline, but a number of the pilots ultimately customized them to fit the needs of their specific information systems.

Guidance

Instructions for the completion of the worksheets can be found in the sample worksheets below. Each page of instructions includes an example – this is a small use-case developed by NIST to illustrate how to include different inputs into the worksheets. The use case is illustrative only and does not reflect the design of any existing system, including those of the NSTIC pilots. The example purposefully includes many privacy flaws.

[50] “Catalyzing the Marketplace: NSTIC Pilot Program,” *supra* Note 14.

Common Issues for Consideration

Over the course of working with the NSTIC pilots, some initial challenges became apparent. These are listed below with some guidance for each.

Unmitigated Risk

In the worksheets, the Summary Issues are the first consolidated assessment where observations that will provide the touch points for identifying problematic data actions are cataloged. This creates a critical juncture for the rest of the analysis – poor summation of the influence of contextual factors on data actions and personal information leads to poor downstream assessment of the potential problems for individuals. The goal of the risk assessment process is to provide a review of unmitigated risk in order to evaluate the comparative effectiveness of mitigating controls. However, pilots using this process sometimes had trouble analyzing existing or planned systems *without* including controls.

This created two challenges:

1. Controls – either implemented or planned – can create an inaccurate assessment of existing or potential risks, and often created temptation for pilots to dismiss potential risks' existence because they were already perceived as resolved. Just because a risk has been mitigated does not mean the risk does not exist at all – and understanding the sources of privacy risk in the system not only helps plan for mitigation strategies but will help agencies understand potential problems of perception, user discomfort, or misunderstanding that could create loss of trust in their system. Without analyzing unmitigated risk, agencies may leave an important output of privacy risk assessment on the table.
2. Because an agency has implemented a control to mitigate privacy risk does not mean it is the most effective control. One benefit of risk assessment is the comparative evaluation of privacy controls. One control might be more costly, but may mitigate risk across a wider number of data actions. Another may be less effective, but affect risk in a way more aligned with the organization's priorities. Some controls may be more appropriate to the current design roadmap for the system than other mechanisms. Effective privacy engineering is about making informed, consistent choices about privacy design that reflect the organization's intentions and priorities, and without comparing the virtues of a variety of choices, that process is short-circuited.

Personal Information

It may be tempting for agencies to consider cataloging personal information only as what is familiar "PII" described in existing PIAs – Social Security Numbers, address, name, date of birth, etc. In order for these worksheets to be effective, agencies should consider personal information very broadly. Any information about an individual or that can be linked to an individual such as behavioral characteristics, should be cataloged in these worksheets. This includes information about session duration, login attempts, behavioral analysis – much of the information considered "metadata" or in system logs that are related to individual users can create privacy problems.

This page is intentionally blank.

Appendix D: Worksheet 1 page 1/3

Worksheet 1 has two tasks to complete:

1. Frame business objectives. Frame the business objectives for the system(s), including the organizational needs served.

2. Frame organizational privacy governance. Frame the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals and other commitments.

Task 1: Frame Business Objectives

1. Describe the functionality of your system(s).

2. Describe the business needs that your system(s) serve.

Appendix D: Worksheet 1 page 2/3

3. Describe how your system will be marketed, with respect to any privacy-preserving functionality.

Task 2: Frame Organizational Privacy Governance

1. Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the system must operate. List any specific privacy requirements.

Appendix D: Worksheet 1 page 3/3

2. Identify any privacy-related principles or other commitments to which the organization adheres (FIPPs, Privacy by Design, etc.).

3. Identify any privacy goals that are explicit or implicit in the organization's vision and/or mission.

4. Identify any privacy-related policies or statements within the organization, or business unit.

This page is intentionally blank.

Appendix D: Use Case page 1/1

The sample information filled out in worksheets 2 and 3 is based on the below use case (which describes a fictional company and situation).

Generic identity service provider (IDP) use case:

ACME IdP service generates a high-assurance identity credential by combining:

- The individual's (social site) online identity;
- An in-person identity proofing event at a trusted third party office (e.g., UPS, FedEx location);
- A One Time Password (OTP) service to be used as a second authentication factor.

The high-assurance credential will subsequently be used to verify the identity of the individual as they attempt to access government benefits.

Appendix D: Worksheet 2 page 1/7

Worksheet 2: Assessing System Design

Purpose: Determining the risk for privacy of a particular data action in an information system requires determining the likelihood that a data action will be problematic (i.e. creates the potential for adverse effectson ind ividuals) and its impact (to be analyzed in worksheet 3). The purpose of this worksheet is to identify and catalog the inputs for this risk analysis. These inputs are the data actions being performed by the system, the personal information being processed by the data action, and relevant contextual factors.

Tasks:

1. Map data processing within the system.
2. Catalog general contextual factors.
3. Catalog specific data actions, personal information being processed and unique contextual factors.

Appendix D: Worksheet 2 page 2/7

Task 1: Map data processing within the system.

Legend

Data action indicator

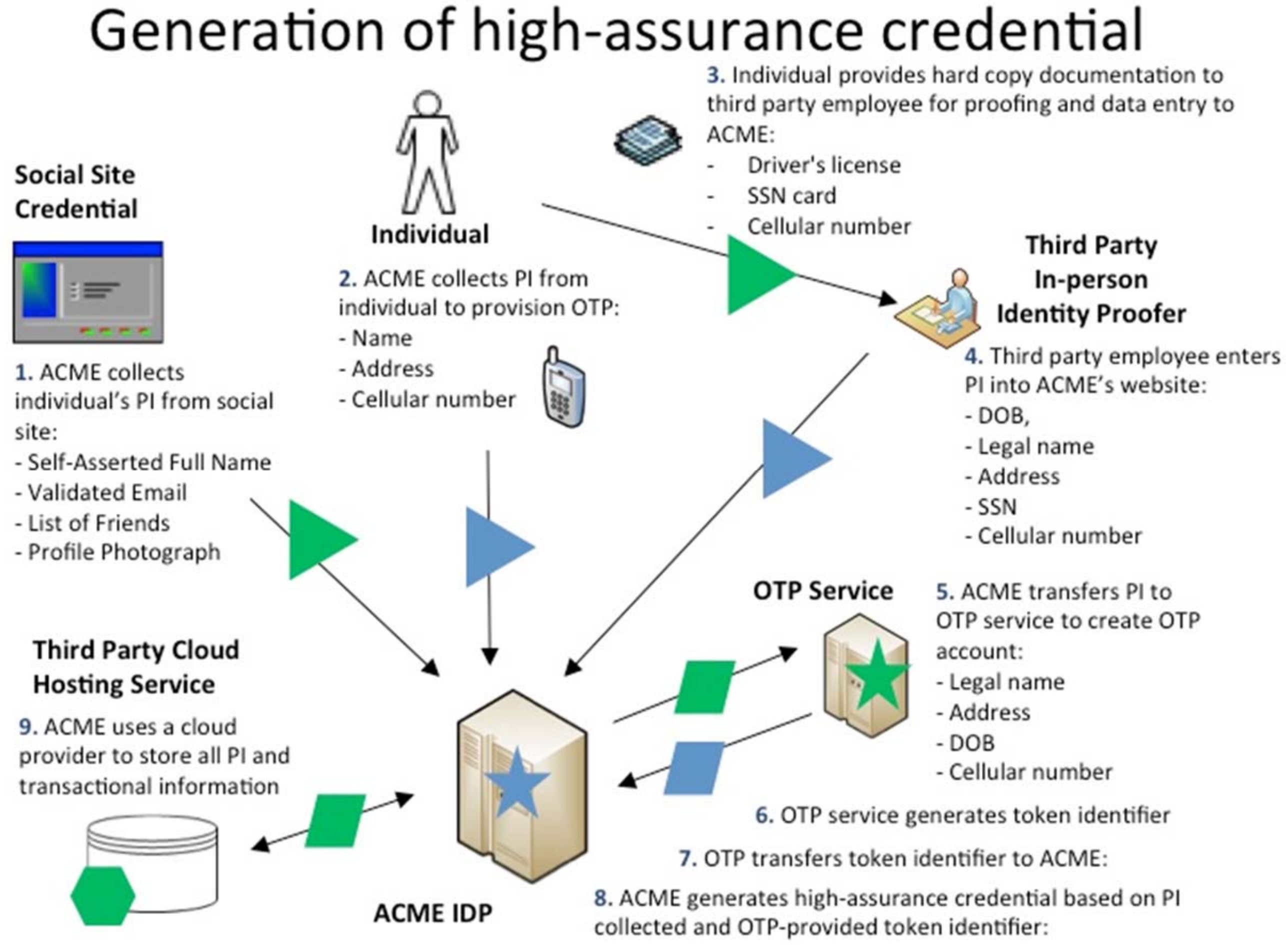
▶	Collection
⬢	Retention/Logging
★	Generation/Transformation
▱	Disclosure/ Transfer
⊗	Disposal

Color coding to depict the operator of the data action

🟦	ACME IDP
🟩	Commercial third-party
🟥	Government third-party

Appendix D: Worksheet 2 page 3/7

Task 1: Map data processing within the system.



Generation of high-assurance credential

Social Site Credential
Individual
Third Party In-person Identity Proofer
OTP Service
Third Party Cloud Hosting Service
ACME IDP

1. ACME collects individual's PI from social site:
- Self-Asserted Full Name
- Validated Email
- List of Friends
- Profile Photograph

2. ACME collects PI from individual to provision OTP:
- Name
- Address
- Cellular number

3. Individual provides hard copy documentation to third party employee for proofing and data entry to ACME:
- Driver's license
- SSN card
- Cellular number

4. Third party employee enters PI into ACME's website:
- DOB,
- Legal name
- Address
- SSN
- Cellular number

5. ACME transfers PI to OTP service to create OTP account:
- Legal name
- Address
- DOB
- Cellular number

6. OTP service generates token identifier

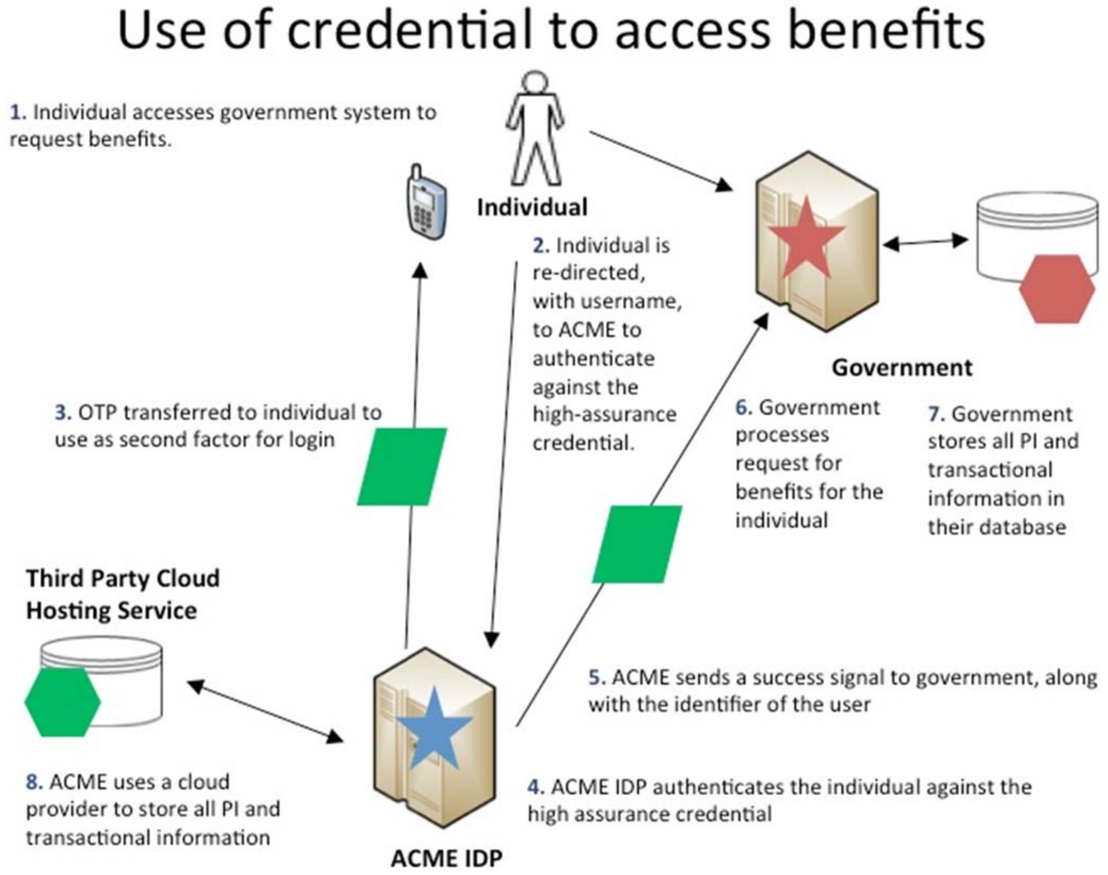
7. OTP transfers token identifier to ACME:

8. ACME generates high-assurance credential based on PI collected and OTP-provided token identifier:

9. ACME uses a cloud provider to store all PI and transactional information

Appendix D: Worksheet 2 page 4/7

Task 1: Map data processing within the system.



Use of credential to access benefits

1. Individual accesses government system to request benefits.

2. Individual is re-directed, with username, to ACME to authenticate against the high-assurance credential.

3. OTP transferred to individual to use as second factor for login

4. ACME IDP authenticates the individual against the high assurance credential

5. ACME sends a success signal to government, along with the identifier of the user

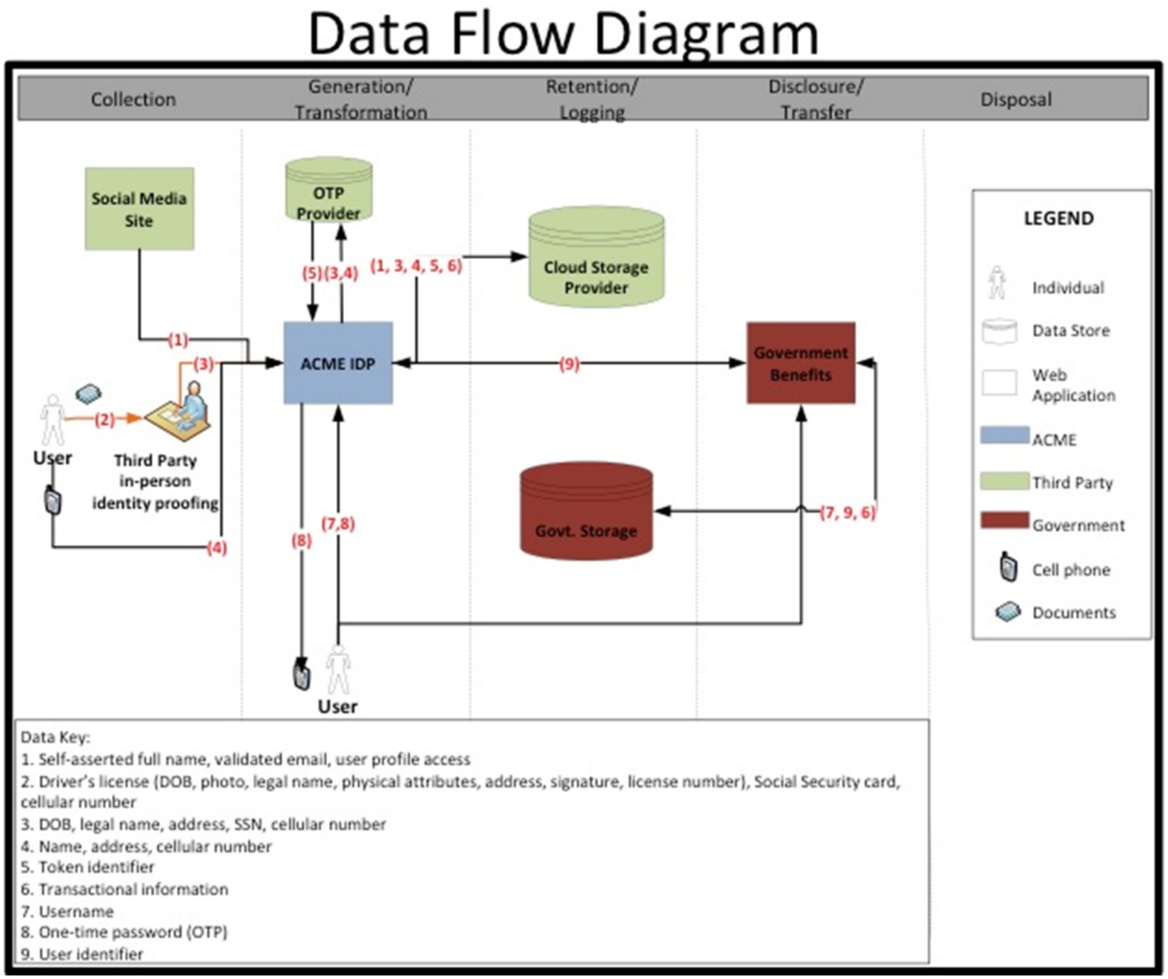
6. Government processes request for benefits for the individual

7. Government stores all PI and transactional information in their database

8. ACME uses a cloud provider to store all PI and transactional information

Appendix D: Worksheet 2 page 5/7

Task 1: Map data processing within the system.



Data Key:
1. Self-asserted full name, validated email, user profile access
2. Driver's license (DOB, photo, legal name, physical attributes, address, signature, license number), Social Security card, cellular number
3. DOB, legal name, address, SSN, cellular number
4. Name, address, cellular number
5. Token identifier
6. Transactional information
7. Username
8. One-time password (OTP)
9. User identifier

Appendix D: Worksheet 2 page 6/7

Task 2: Catalog general contextual factors.

Data Action	Personal Information	Specific Context	Summary Issues
Collection from the Social Media Site	-Self-Asserted Full Name -Validated Email -List of Friends -Profile Photograph	-One-time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between user's social media presence and ACME IDP -Social credential linking is vis ible to user -Linking of social credential simplifies access to government benefits system -User profile may contain information the user considers sensitive -User profile may contain information from other users not participating in the system -User profile includes information unrelated to the purpose and operations of the system -Access to PI is consented by user -Nature of the API: full profile access is granted (by default: name, validated email, profile photograph, and list of friends)	-Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose. -Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider? -How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action? -Will the user understand ACME will have ongoing access to information stored in their social profile? -Will users' social media privacy settings allow this data action?

Appendix D: Worksheet 2 *page 7/7*

Task 2: Catalog general contextualfactors.

Example Contextual Factors
Organizational
System includes both government benefits agency and commercial service providers
Multiple privacy policies governing system
Public perception: high expectation of privacy with government benefits agency, low expectation with social credential provider
Relationships: No pre-existing relationship with ACME IDP, regular interactions with government benefits agency, regular interactions with social credential provider
System
Personal information is not intended to be made public
New system, no history with affected individuals. Low similarity with existing systems/uses of social identity.
Four parties sharing personal information: one public institution, three private
ACME will use 3rd party cloud provider
User
High sensitivity about government benefits provided by system
Users exhibit various levels of technical sophistication
Potential user confusion regarding who "owns" the various segments of each system
20% of users use privacy settings at social provider

This page is intentionally blank.

Appendix D: Worksheet 3 *page 1/6*

Guidance

Likelihood: Probability that a data action will become problematic for a representative or typical individual whose personal information is being processed by the system.

Calculation: Determine on a scale from 1-10 the estimated expected rate of occurrence for each potential problem for individuals whose personal information is being processed per data action.

Prior Worksheet Inputs: Data actions and summary issues from worksheet 2.

Problematic Data Actions Catalog: See *Appendix E.* The catalog may be used as a way to categorize the adverse effects that could arise from the issues or questions highlighted in the Summary Issues column. As noted in Worksheet 2, a summary issue may alleviate, rather than raise concerns about adverse effects. In that case, the summary issue should be scored as 0.

Potential Problems for Individuals Catalog: See *Appendix F*. Problematic data actions may create the potential for more than one type of problem. However, some of the problems may have a higher likelihood of occurrence than others. If the data action ultimately is scored as risky, scoring the problems separately may help pinpoint what type of control would be most effective to mitigate the risk of the data action as a whole.

SAMPLE - Table

Data Actions	Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Likelihood
Collection fromthe social media site	Full social credential profile access (including picture and list of friends)i s not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated revelation	Stigmatization: Information is revealed about the individual that they would prefer not to disclose.	7
			Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage.	2
	Will users understand the eventual high-assurance credentialis controlled by ACME and not by their social credential provider?	-The summaryissue will be associated with another data action.		N/A
	How will perception of the socialmedia organization's privacy practices impact users' willingness to consent to this data action?	-Induced disclosure -Surveillance	Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information.	6

Appendix D: Worksheet 3 *page 2/6*

Guidance

Impact: Cost to the organization of a data action if it became problematic for a representative or typical individual whose personal information is being processed by the system.

Calculation: Determine on a scale of 1-10 the estimated effect of each potential problem for individuals per data action on the business impact factors. The assigned values are added to calculate business impact per potential problem.

Prior Worksheet Inputs: Relevant inputs from Worksheet 1. For example, in considering noncompliance costs, review the legal requirements or obligations identified in the legal environment box.

Business Impact Factors

Noncompliance Costs: Regulatory fines, litigation costs, remediation costs, etc.

Direct Business Costs: Revenue loss from customer abandonment, etc.

Reputational Costs: Brand, damage, loss of customer trust, etc.

Internal Culture Costs: Impact on capability of organization/unit to achieve vision/mission. Consider impact on productivity/employee morale stemming from conflicts with internal cultural values.

Other: Any other costs that an organization wants to consider.

SAMPLE - Table

Data Actions	**Summary Issues**	**Problematic Data Actions**	**Potential Problems for Individuals**	**Business Impact Factors**					**Total Business Impact**
				Noncompliance Costs	Direct Business Costs	Reputational Costs	Internal Culture Costs	Other	
Collection fromthe social media site	Full social credential profile access (including picture and list of friends)i s not necessary for fulfilling operational purpose.	-Appropriation -Induced disclosure -Surveillance -Unanticipated revelation	Stigmatization	7	6	6	4		23
			Power Imbalance	7	6	8	4		25
	How will perception of the socialmedia organization's privacy practices impact users' willingness to consent to this data action?	-Induced disclosure -Surveillance	Loss of Trust	7	6	8	7		28

Appendix D: Worksheet 3 *page 3/6*

Guidance

Risk per Data Action: Apply the risk equation to the outputs of the likelihood & impact tabs to determine the estimated risk per data action. The estimated likelihood per potential problem for individuals per data action is multiplied by its estimated business impact to yield the estimated risk per potential problem. The sum of the estimated risks for each potential problem for individuals is the estimated risk per data action.

SAMPLE - Table

Data Actions	Potential Problems	Likelihood	Business Impact	Risk per Potential Problem	Risk per Data Action
Collection from the social media site	Stigmatization	7	23	161	379
	Power Imbalance	2	25	50	
	Loss of Trust	6	28	168	
DA2	Economic Loss	6	32	192	317
	Loss of Autonomy	5	19	95	
	Exclusion	2	15	30	
DA3	Loss of Trust	6	25	150	577
	Stigmatization	7	36	252	
	Loss of Liberty	5	35	175	
DA4	Loss of Trust	5	48	240	240
DA5	Economic Loss	6	37	222	821
	Loss of Autonomy	5	20	100	
	Power Imbalance	3	25	75	
	Exclusion	8	33	264	
	Stigmatization	4	40	160	
DA6	Loss of Trust	5	22	110	438
	Loss of autonomy	5	32	160	
	Exclusion	6	28	168	
DA7	Loss of Autonomy	8	43	344	659
	Stigmatization	9	10	90	
	Power Imbalance	7	27	189	
	Exclusion	4	9	36	
DA8	Loss of autonomy	4	13	52	514
	Stigmatization	9	32	288	
	Power Imbalance	8	15	120	
	Exclusion	6	9	54	
DA9	Loss of Trust	3	39	117	213
	Loss of Liberty	2	48	96	
DA10	Loss of Trust	4	14	56	161
	Power Imbalance	6	9	54	
	Stigmatization	3	17	51	

Appendix D: Worksheet 3 *page 4/6*

Guidance

System Risk Table: Indicates the estimated risk presented by a data action, its estimated percentage of system risk, and its estimated ranking amongst other data actions. The risk column is the total estimated risk per data action and is colored to facilitate visual prioritization. The percent of system risk column is the estimated risk per data action relative to all other data actions. The rank among the data actions column assigns relative values to the data actions pursuant to their estimated system risk percentage.

SAMPLE – Data Action Risk Prioritization Table

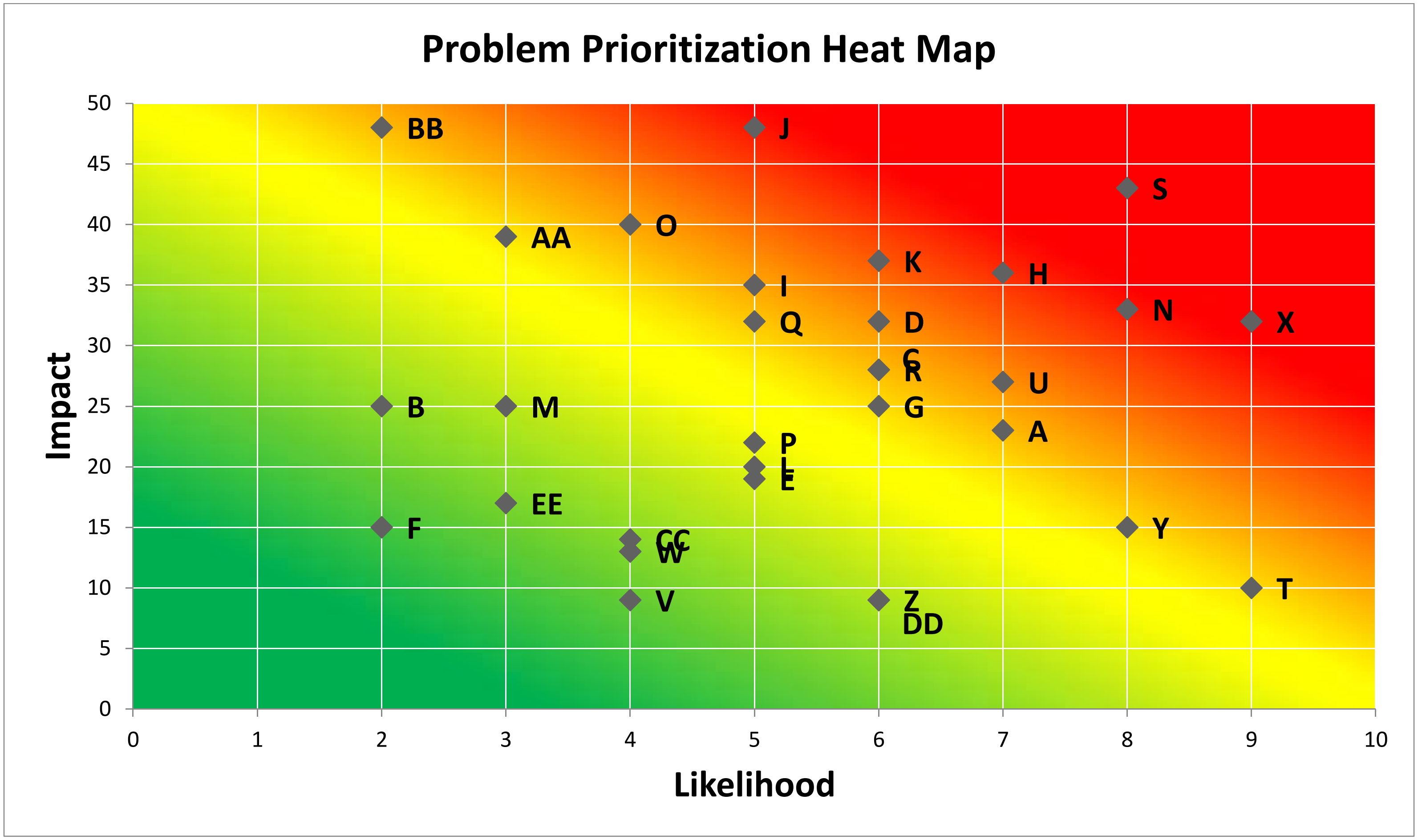
Data Actions	Risk	Percent of System Risk	Rank among Data Actions
Collection from social media site	379	9%	6
DA2	317	7%	7
DA3	577	13%	3
DA4	240	6%	8
DA5	821	19%	1
DA6	438	10%	5
DA7	659	15%	2
DA8	514	12%	4
DA9	213	5%	9
DA10	161	4%	10
Collection from social media site	379	9%	6

Appendix D: Worksheet 3 *page 5/6*

SAMPLE – Two Dimensional Problem Prioritization Table (including 5 top highest likelihood & impact outliers)

Data Actions	Potential Problems	Point Label	Likelihood	Business Impact
Collection from the social media site	Stigmatization	A	7	23
	Power Imbalance	B	2	25
	Loss ofTrust	C	6	28
DA2	Economic Loss	D	6	32
	Loss of Autonomy	E	5	19
	Exclusion	F	2	15
DA3	Loss ofTrust	G	6	25
	Stigmatization	H	7	36
	Loss ofL iberty	I	5	35
DA4	Loss ofTrust	J	5	48
DA5	Economic Loss	K	6	37
	Loss of Autonomy	L	5	20
	Power Imbalance	M	3	25
	Exclusion	N	8	33
	Stigmatization	O	4	40
DA6	Loss ofTrust	P	5	22
	Loss of autonomy	Q	5	32
	Exclusion	R	6	28
DA7	Loss of Autonomy	S	8	43
	Stigmatization	T	9	10
	Power Imbalance	U	7	27
	Exclusion	V	4	9
DA8	Loss of autonomy	W	4	13
	Stigmatization	X	9	32
	Power Imbalance	Y	8	15
	Exclusion	Z	6	9
DA9	Loss ofTrust	AA	3	39
	Loss ofL iberty	BB	2	48
DA10	Loss ofTrust	CC	4	14
	Power Imbalance	DD	6	9
	Stigmatization	EE	3	17

Appendix D: Worksheet 3 *page 6/6*



Problem Prioritization Heat Map

Appendix E: Catalog of Problematic Data Actions

Appropriation: Personal information is used in ways that exceed an individual's expectation or authorization. Appropriation occurs when personal information is used in ways that an individual would object to or would have expected additional value for, absent an information asymmetry or other marketplace failure. Privacy harms that Appropriation can lead to include loss of trust, economic loss or power imbalance.

Distortion: The use or dissemination of inaccurate or misleadingly incomplete personal information. Distortion can present users in an inaccurate, unflattering or disparaging manner, opening the door for discrimination harms or loss of liberty.

Induced Disclosure: Pressure to divulge personal information. Induced disclosure can occur when users feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or privilege to an essential (or perceived essential) service. It can lead to harms such as power imbalance or loss of autonomy.

Insecurity: Lapses in data security. Lapses in data security can result in a loss of trust, as well as exposing individuals to economic loss, and stigmatization.

Surveillance: Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service. The difference between the data action of monitoring and the problematic data action of surveillance can be very narrow. Tracking user behavior, transactions or personal information may be conducted for operational purposes such as protection from cyber threats or to provide better services, but it becomes surveillance when it leads to harms such as power imbalance, loss of trust or loss of autonomy or liberty.

Unanticipated Revelation: Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to stigmatization, power imbalance and loss of trust and autonomy.

Unwarranted Restriction: Unwarranted restriction to personal information includes not only blocking tangible access to personal information, but also limiting awareness of the existence of the information within the system or the uses of such information. Such restriction of access to systems or personal information stored within that system can result in harms such as exclusion, economic loss and loss of trust.

Appendix F: Catalog of Problems for Individuals

Loss of Self Determination

- Loss of autonomy: Loss of autonomy includes needless changes in behavior, including self-imposed restrictions on freedom of expression or assembly.
- Exclusion: Exclusion is the lack of knowledge about or access to personal information. When individuals do not know what information an entity collects or can make use of, or they do not have the opportunity to participate in such decision-making, it diminishes accountability as to whether the information is appropriate for the entity to possess or the information will be used in a fair or equitable manner.
- Loss of Liberty: Improper exposure to arrest or detainment. Even in democratic societies, incomplete or inaccurate information can lead to arrest, or improper exposure or use of information can contribute to instances of abuse of governmental power. More life-threatening situations can arise in non-democratic societies.
- Physical Harm: Actual physical harm to a person.

Discrimination

- Stigmatization: Personal information is linked to an actual identity in such a way as to create a stigma that can cause embarrassment, emotional distress or discrimination. For example, sensitive information such as health data or criminal records or merely accessing certain services such as food stamps or unemployment benefits may attach to individuals creating inferences about them.
- Power Imbalance: Acquisition of personal information that creates an inappropriate power imbalance, or takes unfair advantage of or abuses a power imbalance between acquirer and the individual. For example, collection of attributes or analysis of behavior or transactions about individuals can lead to various forms of discrimination or disparate impact, including differential pricing or redlining.

Loss of Trust

- Loss of trust is the breach of implicit or explicit expectations or agreements about the handling of personal information. For example, the disclosure of personal or other sensitive data to an entity is accompanied by a number of expectations for how that data is used, secured, transmitted, shared, etc. Breaches can leave individuals leave individuals reluctant to engage in further transactions.

Economic Loss

- Economic loss can include direct financial losses as the result of identity theft to the failure to receive fair value in a transaction involving personal information.

Appendix G: Catalog of Contextual Factors

Category	Contextual factors to consider
Organizational	• The nature of the organizations engaged in the system such as public sector, private sector or regulated industry and how this factor might impact the data actions being taken by the system(s). • The public perception about participating organizations with respect to privacy. • The nature and history of user relationships with the organizations participatingin the system(s).
System	• The degree of connections to external systems and the nature of the data actions being conducted by those external systems such as retention, disclosure, or secondary use. • Any intended public exposure of personal information and the degree of granularity. • The nature and history of user interactions withthe system(s). • The degree of similarity between the operational purpose (e.g. goods or services being offered) of this system and other systems that users have interacted with at participating organizations.
Individuals	• What is known about the privacy interests of the individuals whose information is being processed by the system. • The individuals' degree of information technology experience/understanding. • Any demographic factors that would influence the understanding or behavior of individuals with respect to the data actions being taken by thesystem (s).
Data Action	• The duration or frequency of the data actions being taken by the system(s). • How visible the data actions are to the individual. • The relationship between data actions being taken by the system(s) and the operational purpose. For example, in what manner or to what degree is the personal information being collected or generated contributing to the operational purpose? • The degree of sensitivity of the personal information, including particular piecesor the bundle as a whole.

Appendix H: References

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

2. Privacy Act of 1974 (P.L. 107-56), December 1974.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

1. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records Computers and the Rights of Citizens*, June 1973.

2. Federal Trade Commission, Staff Report, *Internet of Things: Privacy and Security in a Connected World*, January 2015.

3. Government Accountability Office, Office of the Inspector General, *GAO's Privacy Program: Opportunities Exist to Further Protect Personally Identifiable Information (PII)*, March 2015

4. Government Accountability Office, Report to Congressional Requesters, *High-Risk Series: An Update*, February 2015.

5. Government Accountability Office, Report to Congressional Requesters, *Actions Needed to Address Weaknesses in Information Security and Privacy Controls*, September 2014.

6. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 2014.

7. The White House, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, May 2014.

8. The White House, Executive Office of the President, *National Strategy For Trusted Identities In Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011.

STANDARDS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

GUIDELINES AND INTERAGENCY REPORTS

1. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.

2. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.

3. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012.

4. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

5. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* March 2011.

6. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

7. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, May 2007.

8. National Institute of Standards and Technology Special Publication 1500-4, *Draft NIST Big Data Interoperability Framework: Volume 4, Security and Privacy*, April 2015.

9. National Institute of Standards and Technology Interagency Report 7628, Revision 1, *Guidelines for Smart Grid Cybersecurity: Volume 2 – Privacy and the Smart Grid*, September 2014.

10. National Institute of Standards and Technology Draft Interagency Report 8053, *De-Identification of Personally Identifiable Information*, April 2015.

11. National Institute of Standards and Technology Internal Report 8054, *NSTIC Pilots: Catalyzing the Identity Ecosystem*, April 2015.